Evaluation of Risk Management Strategies for a Low-Cost, High-Risk Project

Robert Shishko, Ph.D. and Edward J. Jorgensen, CPCM
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

Abstract. This paper summarizes work in progress to define and implement a risk management process tailored to a low-cost, high-risk NASA mission: the Microrover Flight Experiment (MFEX, commonly called the Mats microrover). The tailored risk management process is described along with the extensive data collection, documentation, and quantitative analyses that are being performed. This effort has the explicit purpose of trying, evaluating, and documenting new risk management techniques so as to help not only the MFEX mission, but future missions in the same risk class.

MFEX RISK MANAGEMENT PROCESS AND ACTIVITIES

The Microrover Flight Experiment (MFEX) involves a small, semi-autonomous robotic vehicle to be flown on the Mars Pathfinder (formerly known as MESUR Pathfinder) mission to be launched in 1996. Mats Pathfinder is sponsored by the NASA Office of Space Science (Code S), while the MFEX is sponsored by the NASA Office of Advanced Concepts and Technology (Code C). The MFEX microrover is designed to move away from the Lander part of the Pathfinder spacecraft, image the Lander, place an Alpha Proton X-ray Spectrometer (APXS) on Mars rocks and soil, and perform a variety of technology experiments.

The MFEX risk management activities focused on the following major risk categories: cost, schedule, performance, and operability. Cost risk is considered important because the MFEX has a fixed budget of $25M (RY$) over its entire life cycle. Schedule risk arises because the microrover must be integrated into the Mars Pathfinder spacecraft, which itself must meet the 1996 launch date. Performance risks arise for a variety of reasons: design constraints on volume, mass, and power for both the microrover and its science payload, microrover interfaces with the Pathfinder spacecraft, and use of commercial and Mil-Spec parts. Operability risks arise because of an unknown landed configuration for the Lander, use of new approaches to command, control, and communication, and uncertain environmental conditions.

The general risk management process followed by the MFEX is that described in NHB 7120.5, *Management of Major System Programs and Projects* (Code AD), November 8, 1993, and SP-6 105, *NASA Systems Engineering Handbook* (Code FT), June 1995. The process consists of fear overlapping stages: risk planning, risk identification and characterization, risk analysis, and risk mitigation and tracking. Although the MFEX is too small a project (by criteria set forth in NHB 7120.5) to require a formal Risk Management Plan, the MFEX team developed an informal plan. This plan included the following activities:

Risk Identification and Characterization:
(a) Independent technical assessment
(b) Project team technical assessment
(c) Examining risk tea~platcs/lessons learned documents from previous projects

Risk Analysis:
(d) Cost risk analysis (described in this paper as the Cost Uncertainty Questionnaire)
(c) Operations scenario simulation (described in this paper as the Landed Mission Operations Scenarios)
(f) Failure Modes, Effects, and Criticality Analysis (FMECA)

Risk Mitigation and Tracking:
(g) Contingency planning (described in this paper as the Landed Mission Operations Response Strategies)
(h) Watch list (described in this paper as the MFEX

Risk Management Data Base)

(i) Technical Performance Measure (TPM) tracking and margin management

(j) Schedule float (critical path) tracking and management

Activities (a), (b), and (c) were conducted and completed prior to MFEX Authority 10 Proceed (ATP) to full-scale development. Activities (d), (e), and (g) were first conducted prior to ATP, and will continue throughout the project cycle. The remaining activities were instituted following ATP, but had the benefit of

Figure 1 shows the process for making risk management (unshaded boxes in the figure) integral to the MFEX systems engineering effort. The risk management activities above map into the boxes in Figure 1. For example, the *cost risk analysis* box in the figure is accomplished by performing the Cost Uncertainty Questionnaire. Sometimes, several activities are linked to a particular figure box, as is the case for the *technical risk assessment*. The following example illustrates this process flow. The Mars Pathfinder project has defined its mission needs for the microrover. These are to deploy science instruments and to

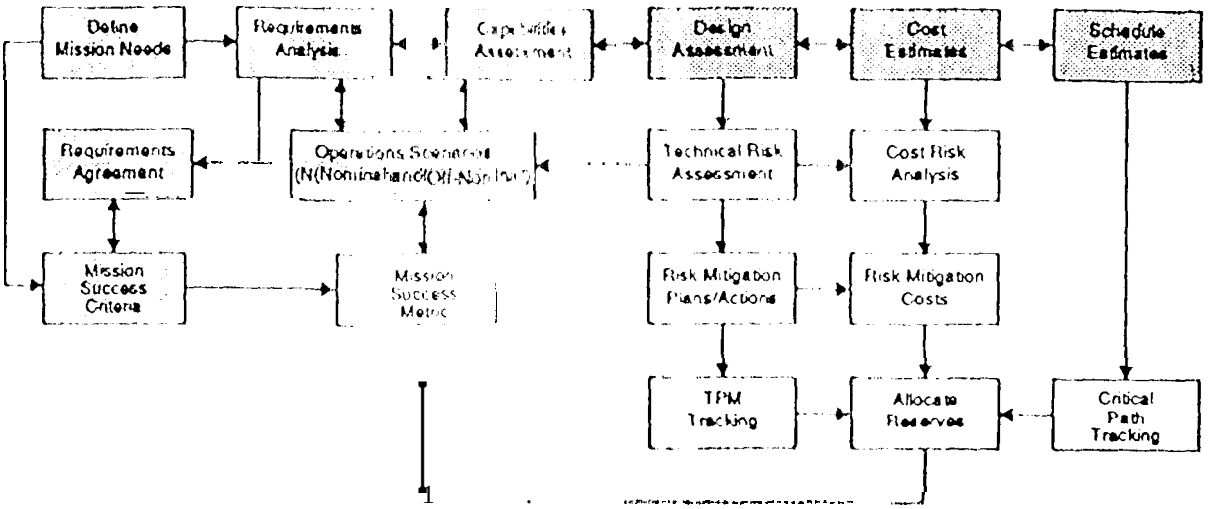

Figure 1 Process for Integrating Systems Engineering and Risk Management

early planning and "start up" work prior to ATP. These activities are also expected to continue throughout the project cycle.

Results and products of the continuing risk management activities are reported periodically to the MFEX team leader. Some, like TPM tracking/margin management results, are updated as changes occur and are reported regularly in the *Microrover Technical Baseline Report*. Others, like the cost risk analysis (which requires more extensive inputs from the subsystem engineers), are conducted prior to major reviews so that the results can be examined in concert with other information. Each new or updated analysis is reported in an MFEX *Risk Management Progress Report*, a total of four of which have been delivered to date under this effort.

image the Lander to determine its condition. Originally, the science desire was for the microrover to deploy a seismometer, and to carry both an Alpha Proton X-ray Spectrometer (APXS) and a neutron spectrometer. A microrover design assessment indicated that a microrover which was capable of fitting within the MFEX cost cap was not capable of carrying even the lightest seismometer. Further, the Mars Pathfinder science budget could not support the neutron spectrometer. Therefore, a capabilities assessment eliminated these two instruments. The requirements analysis led to a requirements agreement between the Mars Pathfinder project and MFEX for a microrover capable of carrying the APXS and placing it on rocks and soil.

In conjunction with the requirements agreement, criteria were established to define MFEX technical

mission success. These criteria are: (1) perform a complete set of technology experiments in one soil type, (2) measure one rock with the APXS and image that rock, (3) produce one full cross section image of the lander, and (4) do two more soil types, and the rock measurement with the APXS, and three more Lander images if possible. Ninety percent technical mission success was assigned to doing (1), (2), and (3) with equal weight to each; an additional ten percent technical mission success was assigned to the extended mission tasks in (4). These criteria established a technical mission success metric.

The requirements analysis was refined (employing landed mission operations scenarios) to determine what functional and performance capabilities were needed by the microrover in order to achieve a scientifically successful mission -- that is, deploy the APXS and perform the other technology tasks described above. As part of the ongoing successive refinement of the microrover design, technical risk assessments were made at increasing levels of detail, and potential failures were identified. For each potential failure, risk mitigation actions were developed, For example, the APXS might not be properly placed on the rock The risk mitigation plan was then amended to include designing and testing prototype APXS deployment mechanisms.

Planning for risk mitigation includes estimating the costs (and schedule implications) of risk mitigation actions, as well as the likelihood that the MFEX life-cycle cost will exceed the cost cap ($25M) because of the identified technical and schedule risk factors. In some instances, TPM tracking provides an indication of the urgency of implementing risk mitigation plans and actions. These assessments are used to allocate MFEX reserves. Allocations are made as problems are encountered For example, after testing the APXS deployment mechanisms (an action in the risk mitigation plan), the likelihood of mechanism failure to properly position the APXS may be reassessed, and reserves allocated to cover the costs of providing for longer APXS operation times to make up for possible misalignment.

Landed mission operations scenarios are the primary tool for assessing the impact of various technical risks on the technical mission success metric. For example, landed mission operations scenarios are used to evaluate the effect of longer APXS operation times on the achievement of other mission objectives, so overall technical mission success can be evaluated With this information, the team leader can determine whether the marginal improvement in technical mission success is worth the additional risk mitigation costs. Just as the systems engineering process is iterative and produces successive refinements of requirements, designs, etc., so is the risk management process. Qualitative. risk assessments are performed first to gain some insights useful for refining the microrover design and operations concept. These then evolve into more quantitative analyses,

SUMMARY OF RISK MANAGEMENT A("1'1 VITIES/STAUS

This section discusses current status of the MFEX with respect to cost, technical performance, schedule, and operability risk.

Cost Risk. The Microrover Cost Uncertainty Questionnaire is the instrument used to collect data on cost risk. The information collected in these questionnaires was intended to : (1) determine cost uncertainty status, (2) identify the elements contributing to the cost uncertainty, (3) estimate the probability of the MFEX's life-cycle cost being less than the $25M (RY$) cost cap, and (4) identify changes in uncertainty over time. It was first administered in July 1993 prior to the Design, Implementation and Cost Review' (DICR), and again in February 1994 prior to the Independent Annual Review (l AR) of March 1994.

Figure 2 graphically illustrates the cumulative distribution function (calf) of MFEX's life-cycle cost at the DICR and IAR. l'hc cdf derived from the initial July 1993 questionnaire indicates that the probability of life-cycle cost being less than or equal to its budget of $25M is 72 percent. Equivalently, the probability of overrunning is 28 percent. A comparison with the cdf derived from the February 1994 questionnaire indicates that while the expected cost (mean) increased, overall cost uncertainty was reduced. This is illustrated by an increase in the slope of the cdf (or equivalently a narrowing of the probability density function.) A third questionnaire is planned to be administered in 1996 at the Assembly, Test, and Launch operations (ATLO) milestone.

Technical Performance Risk: Technical Performance Measures/rMargin Management. Individual Technical Performance Measures (TPMs) have remained relatively stable over time. MFEX is tracking nine TPMs:

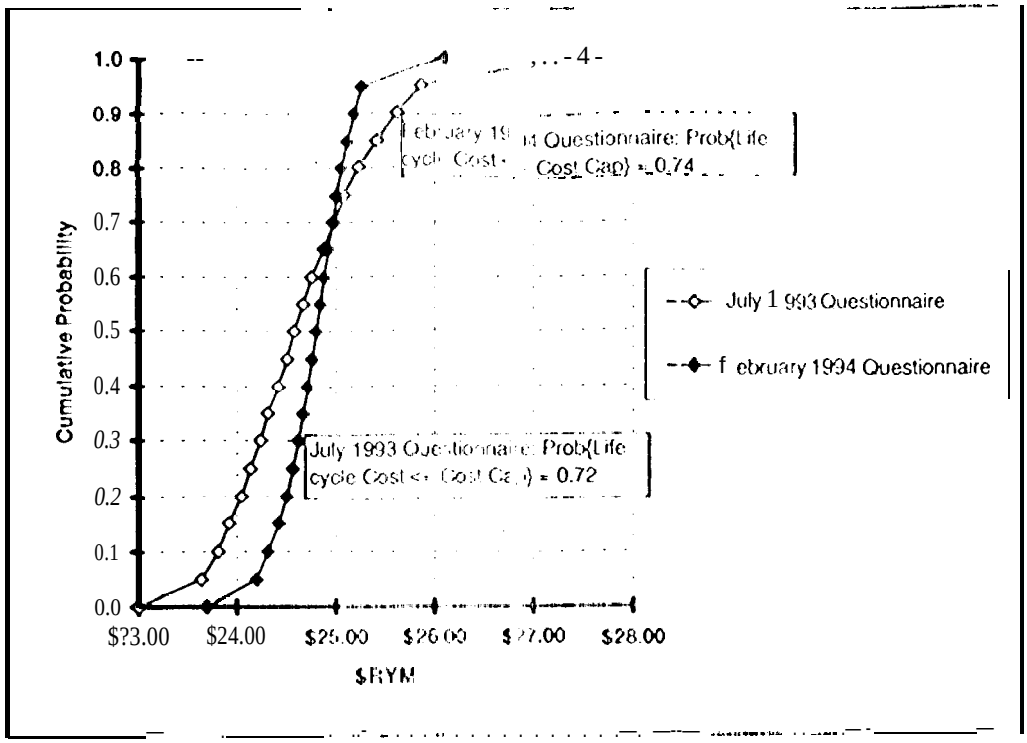

Figure 2 Cost Uncertainty Survey Results

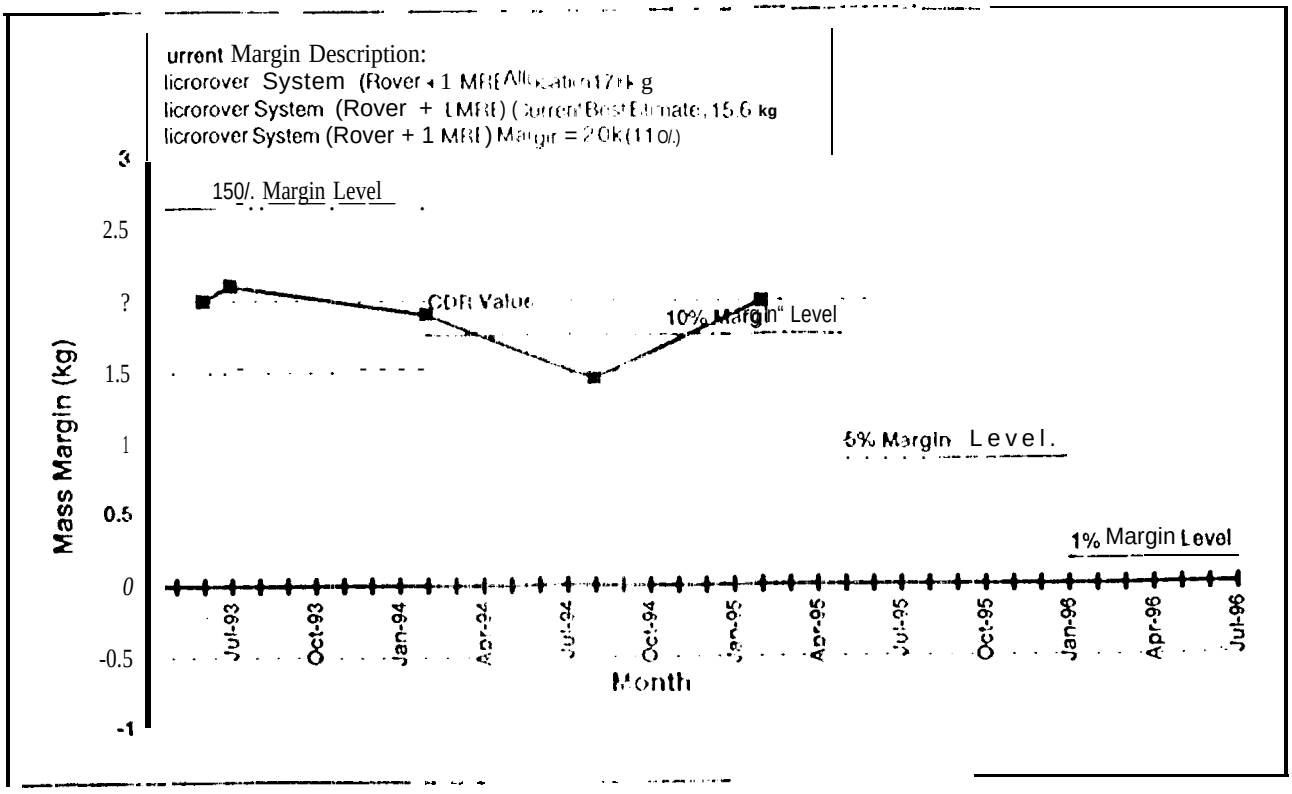

Figure 3 Microrover System (Rover + LMRE) Mass (kg)

- System (Rover -1 LMRE) Mass (kg)
- Warm Electronics Box (Will) Volume (cm^2 x 1 cm)
- Average 1 Driving Power (watts)
- Worst Case Peak Operating Power (watts)
- Sol One Electrical Energy Consumption (watt-hr)
- Development + Ops Thermal Cycles (number of Cycles)
- [Jill Data Flow (Mbits/day)
- I Data Storage - RAM (kbyte)
- Control Memory - PROM (kbyte)

Each TPM is at or above its margin requirement at this time. Figure 3 graphically illustrates the format used for margin display and shows the declining margin requirements "ladder" over time using System Mass (Rover + LMRE) as the example. The remaining TPM charts are displayed in the appendices in References [3] and [4] to this paper. TPM/margin report updates are issued quarterly with incremental updates as the design progresses.

Schedule Risk. In FY 94, schedule management was based upon the use of an integrated network schedule. Ibis was dropped as of April 1994 and replaced with a schedule based upon tracking, the subsystem level Receivables and Deliverables (Rec/Dels). The main reason the integrated schedule could not be sustained was that the activities identified in the schedules were at too detailed a level to be efficiently maintained, given the use of a rapid prototyping development methodology. Furthermore, the USE of numerous commercial parts required that many components be adapted and qualified for use in a space and Mars environment. The schedule required for this was difficult to anticipate, as the history conveyed below suggests.

The schedule status as of February 20, 1995, based on the July 1994 Baseline Rec/Del plan, reveals 36 actual completed deliverables out of 54 planned completions (see Figure 4). This means that only 67% of the planned milestones have actually been Completed, Looking at schedule slips from a variety of perspectives basically reveals that MFEX is currently running from 4 to 5 weeks behind the July 1994 Baseline schedule. The average number of (work)days late for all milestones is 25 days. The average days late for all *critical path* milestones is 22 days. The average days slipped for completed critical path milestones is 17 days, The aver-age days slipped for the three currently open items is 35 days. The main critical items are the deliveries for the System Integration Test I. I (SIM) vehicle, which have so far slipped 21 days to May 15, 1995. This is approximately equivalent to a nine percent schedule slip as measured from April 1994 through the end of February 1995.

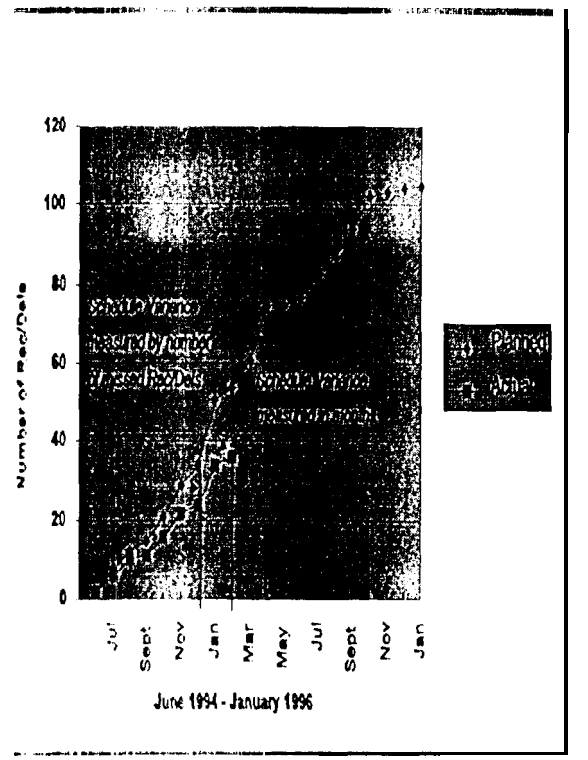

Figure 4. MFEX Ret/Del Accomplishment: Planned Versus Actual

The schedule reserve in the beginning, of FY94 was originally three months. As of December 1994, the remaining system-level schedule reserve was one month. It appears that MFEX currently has no schedule reserve except for possible. float inherent in some individual deliverables. Given that in the past year an overall schedule slip of nine percent has been observed, it should be expected that some additional slips will occur in the future. Because MFEX is a high-risk mission, there is some flexibility in how the microrover is tested. Therefore, as part of a contingency plan, a number of subsystem level tests tests have been identified for deletion from the schedule, and a schedule recovery plan is currently being implemented

The main MFEX schedule drivers have been the Mobility Subsystems, Warm Electronics Box (WEB) and the Navigation and Control Subsystems electronic boards. Since April 1994, the WEB has undergone a major redesign to an insulation material of solid silica aerogel instead of one consisting of an aluminum-based powder sandwich. In some early vibration tests it was found that the powdered insulation shifted resulting in undesirable temperature gradients. The result was a redesign with additional supporting analysis that delayed the build of a WEB engineering model by three (3) months. Additional assembly-level thermal and vibration tests were also scheduled in order to verify the design and the aerogel insulation material, which had not previously been used as thermal insulation. Consequently, the WEB design was not ready for the beginning of the SIM build until December 1994. The refitting of the Rocky 4 development/test vehicle into a software development model (SDM) was scheduled to be completed and ready for sandbox testing by September 1994 with the addition of a computer and associated electronics in a printed circuit board package. Delays in the development of this set of electronics boards caused by parts availability, parts substitution (i. e., commercial equivalent for unavailable flight parts) and fabrication delays resulted in the boards being first available in December 1994.

The Rocky 4.6 vehicle was established as a SDM in January 1995. To provide an environment for software development, a version of these electronics in a wirewrap breadboard with commercial part equivalents was produced and integrated with the Rocky sensors and chassis (creating Rocky 4.5). Testing and evaluation of this substitute added further delay to the printed circuit board production while keeping other control and navigation subsystem developments on schedule. Schedule impacts have occurred in general because of time spent (1) searching for substitute parts/vendors that could meet schedule requirements, (2) evaluating the appropriateness of certain commercial parts, and (3) identifying and accommodating vendor order and lead times for parts needed for prototype board builds.

Some lessons learned related to schedule management of missions like MFEX are already apparent. Due to the rapid changes that arise in plans in a task using rapid prototyping, scheduling must be kept at a fairly high level so that the cost of updating the network schedule database is not burdensome. A better approach to schedule management for tasks like MFEX is (1) finalize the Rec/Del list, (2) agree on the inter-subsystem and external product interfaces, and then (3) construct a high-level integrated schedule. The Rec/Del list is currently MFEX's only formal schedule management technique. However, it is not possible to discern from a Rec/Del schedule what the real schedule drivers are as these lie at least one level below the subsystem external deliverables.

A second lesson learned is that a standard schedule management tool must be identified from the very beginning of the task. Lastly, very large schedule margins need to be established in the early phases of the Class D project to allow for the extensive schedule uncertainty associated with the testing requirements of commercial parts. How large is not yet clear, but three months of margin as late as the beginning of FY94 was not enough.

Operability Risks. The primary tool used to devise sensible operations concepts for the microrover is a deterministic simulation of the events that form *landed mission operations scenarios*. These simulations, which are embodied in Excel spreadsheets, are used to estimate how many sols it requires to achieve the mission success criteria defined in Section 1.2 above.

The Landed Mission Risk Assessment Survey, performed on a one-time basis in August 1993 and reported in the first Risk Management Progress Report, identified the highest risks to MFEX mission success. (See Section 2.2, Table 2.1 in *Risk Management Progress Report*, JPL D-11181-1, December 1993.) For all of the top risks, potential operational response/recovery strategies were developed as part of the risk mitigation effort. The logical step is to insert off-nominal conditions into the deterministic scenario simulations, and calculate the effects on the landed mission timeline taking into account any operational response/recovery strategies.

Of the top 15 risks, four involve the failure of some portion of the uplink/downlink capability on the microrover or Mars Pathfinder lander (e.g., the lander HGA could fail to deploy), and eight involve physical obstructions to microrover deployment. The operations response/recovery strategies for the former involve (1) pre-stored command sequences, which are activated autonomously, and (2) workarounds utilizing alternative means to communicate or collect data. In the latter set of risks, response/recovery strategies involve slowing operations to allow more time to take and analyze images before attempting deployment. In any case, the amount of time needed to complete various mission tasks increases, which in turn affects

The main MFEX schedule drivers have been the Mobility Subsystems, Warm Electronics Box (WEB), and the Navigation and Control Subsystems electronics boards. Since April 1994, the WEB has undergone a major redesign to an insulation material of solid silicon aerogel instead of one consisting of an aluminum-based powder sandwich. In some early vibration tests, it was found that the powdered insulation shifted resulting in undesirable temperature gradients. The result was a redesign with additional supporting analysis that delayed the build of a WEB engineering model by three months. Additional assctnbly-level thermal and vibration tests were also scheduled in order to verify the design and the aerogel inhalation material, which had not previously been used as thermal ill~ul.ill! m Consequently, the WEB design was not ready for the beginning of the SIM build until December 1991, The refitting of the Rocky 4 development/test vehicle into a software development model (SDM) was scheduled to be completed ant] ready for sandbox testing by September 1994 wi(h the addition ofa computer and associated electronics in a printed circuit board package. Delays in the development of this set of electronics boards caused by parts availablility, parts substitution (i.e., commercial equivalent for unavailable flight parts) and fabrication delays resulted in the boards being first available in December 1994.

The Rocky 4.6 vehicle was established as a S1)M in January 1995. '1'0 provide an environment for software development, a version of these electronics in a wirewrap brassboard with commercial part equivalents \vas produced and integrated with the Rocky sensors and chassis (creating Rocky 4.5). Testing and evaluation of this substitute added further delay to the printed circuit board production while keeping other control and navigation subsystem developments 011 schedule. Schedule impacts have occurred in general because of time spent (1) searching for substitute parts/vendors that could meet schedule requirements, (2) evaluating the appropriateness of certain commercial parts, and (3) identifying and accommodating vendor order lead times for parts needed for prototype board builds.

Some lessons learned related 10 schedule management of missions like MFEX are already apparent. Due to the rapid changes that arise in plans in a task using rapid prototyping, scheduling must be kept at a fairly high level so that the cost of updating the network schedule database is not burdensome. A better approach to schedule management for tasks like MFEX is (1) finalize the Rec/Del list, (2) agree on the inter-subsystem and external product interfaces and then (3) construct a high-level integrated schedule. The Rec/Del list is currently MFEX's only formal schedule management technique. However, it is not possible to discern from a Rec/Del schedule what the. real schedule drivers are as these lie at least one level below the subsystem external deliverables.

A second lesson learned is that a standard schedule management tool must be identified from the very beginning of the task. Lastly, very large schedule margins need to be established in the early phases of the Class 1) project to allow for the extensive schedule uncertainty associated with the testing, requirements of commercial parts. } low large is not yet clear, but three months of margin as late as the beginning of FY94 was not enough.

Operability Risks. The primary tool used to devise sensible operations concepts for the microrover is a deterministic simulation of the events that form *landed mission operations scenarios*. These simulations, which are embodied in Excel spreadsheets, are used to estimate how many sols it requires to achieve the mission success criteria defined in Section 1.2 above.

'1 he Landed Mission Risk Assessment Survey, performed 011 a one-time basis in August 1993 and reported in the first Risk Management Progress Report, identified the highest risks to MFEX mission success. (See Section 2.?, Table 2.1 in Reference [3].) For all of the top risks, potential operational response/recovery strategies were developed as parf of the risk mitigation effort 'f he logical step is to insert off-nominal conditions into the deterministic scenario simulations, and calculate the effects on the landed mission timeline taking into account any operational response/recovery strategies.

Of the top 15 risks, four involve the failure of some portion of the uplink/downlink capability on the microrover or Mars Pathfinder lander (e.g., the lander HGA could fail to deploy), and eight involve physical obstructions to microrover deployment. The operations response/recovery strategies for the former involve (1) pre-stored command sequences, which are activated autonomously, and (2) workarounds utilizing alternative means to communicate or collect data. In the latter set of risks, response/recovery strategies involve slowing opt] ations to allow more time to take and analyze images before attempting deployment. In any case, the amount of time needed to complete various mission tasks increases, which in turn affects

the microrover's ability to complete [illegible] criteria due to its decreasing reliability.

The focus of effort by the MFEX team since Apr 1994 has been on the development of the operation response/recovery strategies for sol 1 and sol 2. In May 1995, the nominal and off-nominal landed mission operations scenarios were presented showing the pre-stored sequences to be used in the event of uplink/downlink failures. In principle it is possible to calculate the probability density of the landed mission success function, though at this time more work and analysis are needed to do so. Additional work on the landed mission success probability is planned for FY96.

MFEX Risk Management Database/Test Database

The MFEX Risk Management Database is the primary means of documenting all identified MFEX risks, describing the applied mitigations, and monitoring their subsequent effectivity. When a mitigation response involves a test, a Test Database record is created and added to the Test Database. An analysis of the subsytem data so far revealed that for a relatively low cost, a dramatic decrease in the expected failure rate was achieved. The preliminary results discussed below exclude the cost of software testing, which was performed by the Navigation and Control Subsystem.

Figure 5 displays the estimate of the probabilities of failure for three subsystems at the beginning of the project and near the completion of the development tests. For each of the subsystems, the initial probability of failure is derived from the CogEs *subjective* estimate that a subsystem component would fail a specific test (e.g. thermal, vibration, etc.). The probability of failure at the completion of the development tests is based on the CogEs subjective estimate that a subsystem component would survive the environment being tested *on Mars*. The component-level probabilities were combined (assuming independence) to obtain the subsystem-level probability of failure. At the start of the project the probabilities of failure ranged from 94% for the Mobility and Thermal Subsystem to 99% for the Navigation and Control Subsystem. It was so high because of the use of numerous commercial parts which were basically unknown commodities. By the end of development testing, the subsystems' probabilities of failure on Mars

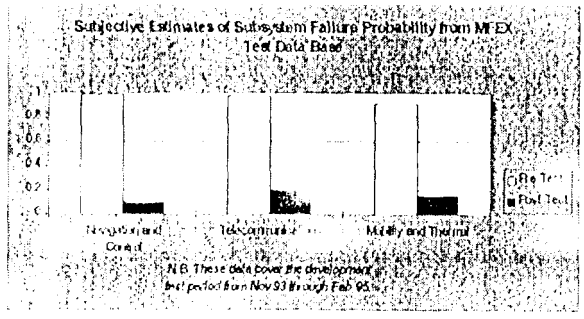

Figure 5. Pre-and Post Test Subsystem Failure Probability Estimates

had fallen to a range of 10% to 20%. The only reason the probability of failure is still this high is that some component-level testing was slipped to subsystem-level acceptance and qualification testing in order to save money and schedule. It is expected that these tests will verify the performance of the subsystem components and further lower the probabilities of failure. For example, the Telecommunications Subsystem must repackage the modem to survive the vibration environment. The formal vibration test will be performed as part of the acceptance test activities, which will actually be conducted by the Mobility and Thermal Subsystem.

FUTURE WORK

Future work will continue the activities reported above, including another Cost Uncertainty Questionnaire, TPM tracking, Rec/Del tracking, and MFEX Risk Management Database/Test Database expansion. New efforts will be focused on the microrover Failure Modes, Effects, and Criticality Analysis (FMECA) and its connection to operability risk. Specifically, work has begun on a model to relate failure rates to the (stochastic) thermal cycling that occurs during the Martian sol. This will be integrated with the landed mission operations scenarios so that probabilistic mission success metrics can be calculated as a function of time following microrover deployment.

REFERENCES

NASA Headquarters, *Management of Major System Programs and Projects*, NHB 7120.5, November 1993.

NASA Headquarters, *NASA Systems Engineering Handbook*, SP-610S, June 1995.

Jorgensen, Ed and Robert Shishko, "Mitt orover 1 light Experiment: Risk Management Progress Report C, JPL Internal Document 1>-11181-1, Jet Propulsion laboratory, Pasadena, CA, 2,1 December 1993

Jorgensen, Ed and Robert Shishko, "Microrover 1 light Experiment: Risk Management Progress Report CDR Update", JPL Internal Document 1)-1 1] 81.', Jet Propulsion Laboratory, Pasadena, CA, 28 April **1994.**

BIOGRAPHY

Robert Shishko attended M.I.T. and Yale University, and serves as a senior economist at JPL, and part-time on the faculty of the International Space University. He is a principal author of the NASA Systems Engineering Handbook.

Edward Jorgensen attended the University of Arizona, earning degrees in Mechanical Engineering and Economics. He serves as a member of the technical staff at JPL's Project Design Center.

The research described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration